BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 100 63 059.6

Anmeldetag: 18. Dezember 2000

Anmelder/Inhaber: Siemens AG, München/DE

Bezeichnung: Schutz von Textdaten und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln

IPC: G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 7. November 2001
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Sieck

A 9161
03/00
EDV-L

Beschreibung

Schutz von Textdaten und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln

Im Zuge der Verbreitung von XML als Speicherformat für Daten geht die Möglichkeit, Daten und Programme gegen Analyse und Benutzung durch Unbefugte zu schützen verloren.

Das Problem ist neu und wurde bisher nicht gelöst.

Durch die Integration einer Entschlüsselung in einen Preprozessor unter Verwendung von asymmetrischen Schlüsseln (siehe PGP) ergeben sich folgende Vorteile:

a) Die bekannten Routinen für Ver- und Entschlüsselung wandelt von ASCII-Text in ASCII-Text. Die verschlüsselten Bereiche lassen sich also genauso speichern und transportieren wie die unverschlüsselten Bereiche und bieten damit eine ideale Integration in XML.

b) Durch das Textformat lassen sich auch Teile eines Textes verschlüsseln. Man kann also den Kopf eines Programmes mit Defines zum Anpassen unverschlüsselt lassen, den Körper mit den Funktionen aber schützen.

c) Der Lieferant einer Anwendersoftware (z.B. Compiler oder Projektiertool) gibt dieser ein eigenes Schlüsselpaar. Der Lieferant speichert den Public Key mit den Kundendaten des Anwenders. Jetzt kann der Lieferant Bibliotheken für bestimmte Kunden mit deren Public Key verschlüsseln und über beliebige Kanäle an diese Kunden übermitteln. Jegliche Kopie ist sinnlos, da die Bibliothek ausschließlich auf der Anwendung des vorgesehenen Kunden entschlüsselt werden kann. Ein Lizenzsystem ist damit leicht realisierbar.

d) Die verschlüsselten Texte sind nicht analysierbar. Ein Know How Diebstahl ist nicht möglich.

Die Kombinierung der an sich bekannten Verfahren ist neu.

Für die Realisierung des Verfahrens wird im Engineering System ein Export- und ein Import-Mechanismus für Projektierdaten im XML-Format verwendet. Damit werden Probleme bei Versionsübergängen, Dokumentation und Analyse gelöst.
Eine Bibliothek auf Basis der exportierten XML-Daten bringt weitere Vorteile.

Durch die Integration einer asymmetrischen Entschlüsselung in einen Preprozessor des Compilers lassen sich Programmteile gegen Missbrauch schützen, ohne den Compiler selber zu ändern. Der Preprozessor läuft nur bei der Erzeugung des binären Codes für das Zielsystem. Der Programmeditor benötigt auch keine Änderung. Es wird nur der Verschlüsselte Text angezeigt.
Eine Integration einer asymmetrischen Verschlüsselung als Postprozessor in den Export der Parameter ermöglicht auch den Schutz der projektierten Daten. Der Import erhält dann ebenfalls einen Preprozessor für die Parameter.

Probleme bei der Vermarktung von werden durch das erfindungsgemäße Verfahren und den erfindungsgemäßen Mechanismus gelöst. Mit der bisherigen Technik ist ein Know How Schutz nicht möglich. Jeder kann die XML-Daten lesen und die enthaltene Parametrierung und Programme lesen, kopieren und für eigene Zwecke einsetzen.

Patentansprüche

1. Verfahren zur Verschlüsselung und Entschlüsselung von Textdaten und Programmen, unter Verwendung eines Public Key,
gekennzeichnet durch eine Untermenge folgender Merkmale:
- Beschreibung der Daten und Programme in XML,
- Verwendung von asymmetrischen Schlüsseln
- Verschlüsselung und/oder Entschlüsselung durch einen Pre-Processor
- Gleichbehandlung von verschlüsselten und unverschlüsselten Bereichen bei der Speicherung.

2. System zur Verschlüsselung und Entschlüsselung von Textdaten und Programmen, unter Verwendung eines Public Key,
gekennzeichnet durch eine Untermenge folgender Merkmale:
- Beschreibung der Daten und Programme in XML,
- Verwendung von asymmetrischen Schlüsseln
- Verschlüsselung und/oder Entschlüsselung durch einen Pre-Processor
- Gleichbehandlung von verschlüsselten und unverschlüsselten Bereichen bei der Speicherung.

Anhang zur Erfindungsmeldung:
Schutz von Textdateien und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln